IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Hashem Mohammad Ebrahimi

Title: BROKERING STATE INFORMATION AND IDENTITY AMONG USER AGENTS, ORIGIN SERVERS, AND PROXIES

Docket No.: 1565.035US1
Filed: January 18, 2000
Examiner: Carl G. Colin

Serial No.: 09/484,691
Due Date: April 6, 2006
Group Art Unit: 2136

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

X Appeal Brief including authorization to charge Deposit Account 19-0743 in the amount of $500.00 to cover the appeal fee (25 pgs.).
X Return postcard.

Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: _____
Atty. Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 6 day of April, 2006.

Peter Rebuffoni
Name

_____
Signature

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

Page

1. REAL PARTY IN INTEREST 2

3. RELATED APPEALS AND INTERFERENCES 3

3. STATUS OF THE CLAIMS 4

4. STATUS OF AMENDMENTS 5

5. SUMMARY OF CLAIMED SUBJECT MATTER 6

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 9

7. ARGUMENT 10

8. SUMMARY 15

CLAIMS APPENDIX 16

EVIDENCE APPENDIX 23

RELATED PROCEEDINGS APPENDIX 24

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Hashem M. Ebrahimi Examiner: Carl G. Colin

Serial No.: 09/484,691 Group Art Unit: 2136

Filed: January 18, 2000 Docket: 1565.035US1

BROKERING STATE INFORMATION AND IDENTITY AMONG USER AGENTS, ORIGIN SERVERS, AND PROXIES

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on February 3, 2006 and received by the Patent Office on February 6, 2006, from the Final Rejection of claims 1-31 of the above-identified application, as set forth in the Final Office Action mailed on November 3, 2005.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of 500.00 which represents the requisite fee set forth in 37 C.F.R. § 41.2(b)(2). Appellant respectfully requests consideration and reversal of the Examiner's rejections of pending claims.

04/11/2006 AWONDAF1 00000056 190743 09484691
01 FC:1402 500.00 DA

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, Novell, Inc. as evidenced by the assignment recorded from the inventors to Novell, Inc. on January 18, 2000 at Reel 010518, Frames 0670 - 0674.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

The present application was filed on February 3, 2006 with claims 1-31. A Final Office Action (hereinafter "the Final Office Action") was mailed November 3, 2005. Claims 1-31 stand twice rejected, remain pending, and are the subject of the present Appeal.

4. STATUS OF AMENDMENTS

No amendments have been made subsequent to the Final Office Action dated November 3, 2005.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Some aspects of the present inventive subject matter include, but are not limited to, methods, systems, transparent proxy servers, and media for brokering state information and identity among agents, servers, and proxies.

According to an aspect, a method for brokering state information exchanged between computers using at least one protocol above a transport layer is provided, as illustrated in FIG. 7 and its related discussion in the specification. A transparent proxy receives a request from a client that is requesting a resource of an origin server, wherein the transparent proxy is unknown to the client. See, page 20 lines 9-19. The client request is then redirected from the transparent proxy to a policy module. See, page 21 lines 3-5. Next, the transparent proxy obtains policy enforcement data, wherein the policy enforcement data is received from the policy module and wherein the policy module and the transparent proxy reside within a same environment. See, page 22, lines 12-15; also see, FIG. 6 item number 502 and 608 and related discussion in the specification. Finally, a policy state token is generated at the transparent proxy in response to the policy enforcement data and the policy state token is transmitted from the transparent proxy to the client, wherein the policy state token is used as an authentication of the client to the transparent proxy for subsequent interactions between the client and the transparent proxy. See, page 23 lines 6-23.

In another aspect, a transparent proxy is provided, as illustrated in FIGS. 5 and 6 and its related discussion in the specification. The transparent proxy 502 includes a memory 600 configured at least in part by a transparent proxy process (page 17 last line and continuing to page 18 line 1) and a processor 602 for running the transparent proxy process (page 18 lines 7-12). The transparent proxy also includes at least one link 604 for networked communication between the transparent proxy process, one the one hand, and a client computer 504 and an origin server 102, on the other hand (page 18 lines 13-14). The transparent proxy 502 also includes a policy module identifier 606 which identifies a policy module 608 (page 18 lines 17-18) that grants or denies authorization of proxy

services to the client computer 504 by acquiring policy enforcement data and attempting to authenticate the client computer 504 to the transparent proxy service in response to the policy enforcement data (page 19 lines 1-6), and wherein the client computer 504 directs a request for a resource to an origin server 102 and the request is intercepted by the transparent proxy process (page 20 lines 13-19), which is unknown to the client computer 504 (page 20 lines 11-19), and used to determine the policy module identifier 606 which identifies the policy module 608, and wherein the policy module 608 authenticates the client computer 504 to the transparent proxy process for subsequent interactions between the client computer 504 and the transparent proxy process (page 26 lines 5-19), and wherein the policy module 608 processed within a same environment as the transparent process (page 22 lines 12-15; FIG. 6 item numbers 502 and 608; and FIG. 7 and related discussion).

In still another aspect, a distributed computer system is provided. See Fig. 10 and related discussion beginning on page 30; also see FIG. 7 and its related discussion. The system includes a first signal 1002 including a redirection command which specifies the policy module 608 address as a redirection target (page 30 lines 20-23). The system also includes a second signal 1004 including a redirection command which specifies the transparent proxy server address as a redirection target and also including policy enforcement data which grants or denies authorization for the client to use a service of the transparent proxy server, and wherein the transparent proxy server controls access to the service based on client authentication to the proxy service achieved through the policy enforcement data (page 31 lines 4-11), the first and second signal originating within a same environment that is external to the client (see FIG. 6 item numbers 502, 504, and 608), and wherein the transparent proxy server is unknown to the client (page 20 lines 11-19).

In yet another aspect, a storage medium is provided. See FIG. 7 and related discussion. The medium includes instructions (page 17 lines 8-16) that receive a request at a transparent proxy from a client that requests a resource of an origin server, wherein the transparent proxy is unknown to the client. See, page 20 lines 9-19. The instructions also redirect the client request from the transparent proxy to a policy module (page 21

lines 3-5) and obtains, at the transparent proxy, policy enforcement data provided by the policy module (page 22 lines 12-15), the policy enforcement data grants or denies authorization for the client to access the resource through the transparent proxy (page 24 lines 19-21), wherein the policy enforcement data is directed to authenticating the client to the transparent proxy and the transparent proxy vends access to the resource (page 26 lines 13-19), and wherein the policy module and the transparent proxy execute within a same environment that is external to the client. See, FIG 6 item numbers 502, 504, and 608 and related discussion.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-3, 7-8, 9-17, and 20-28 were rejected under *35 USC § 103(a)* as being unpatentable over U.S. Patent 6,401,125 (hereinafter "Makarios") in view of U.S. Patent 6,003,084 (hereinafter "Green").

B. Claims 4, 6, 18, 19, 29, and 30 were rejected under *35 USC § 103(a)* as being unpatentable over Makarios in view of Green and in further view of U.S. Patent Publication 2002/0007317 (herein after "Callaghan").

C. Claim 5 is rejected under *35 USC § 103(a)* as being unpatentable over Makarios in view of Green and in view of Callaghan and in still further view of U.S. Patent 5,805,803 (hereinafter "Birrell").

D. Claim 31 is rejected under *35 USC § 103(a)* as being unpatentable over Makarios in view of Green and in further view of U.S. Patent 6,728,884 (herein after "Lim").

7. ARGUMENT

A) The Applicable Law under 35 U.S.C. §103(a)

To sustain a rejection under 35 U.S.C. 103, references must be cited that teach or suggest all the claim elements. M.P.E.P. § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); *Schenck v. Nortron Corp.*, 713 F.2d 782, 218 USPQ 698 (Fed. Cir. 1983); *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985); MPEP § 2141.02.

Further, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143. The Examiner must avoid hindsight. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). The Office Action must further provide specific, objective evidence of record for a finding of a suggestion or motivation to combine reference teachings and must explain the reasoning by which the evidence is deemed to support such a finding. *In re Sang Su Lee*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002).

B.) Primary References Cited

Makarios discloses techniques for customizing web viewing for a user by means of a proxy that includes presentation attributes from a particular user that is independent of any particular service that user may access over the Internet. In Makarios, a client browser houses a cookie for a proxy, the proxy processes requests by the client to Internet services and access the cookie before forwarding the requests to the services. The cookie identifies the client to the proxy and permits the proxy to customize the experience of the client with the Internet services, even if the client has never interacted with the Internet

services. See, Makarios, col. 4 lines 30-48. Makarios requires the client to be registered or initially configured to interact with the proxy. See, Makarios, col. 5 lines 10-18. A first time the client interacts with the proxy it configures or registers with the proxy via a signup form.

Green is directed to techniques for auditing and validating connections between applications. To do this, Green looks at connected applications engaged in communications with one another and validates them against access lists. If a connection is not permissible, the connection is terminated. If a connection is permissible, it is re-established using a transparent process as an intermediary. Green asserts to provide improved firewall security.

C. The rejections of the independent claims 1, 14, 23, and 27 under *35 USC § 103(a)* in view of a Makarios and Green combination:

The Examiner asserts that it is proper to combine the Makarios and Green combination and that such combination renders Applicant's independent claims obvious. The Examiner is relying on Makarios for the bulk of the teachings in the independent claims and relies on Green for the teaching of a transparent proxy.

Applicant asserts that such combination is in error. The teaching in Makarios specifically requires a forward proxy. Thus, this reference teaches away from Applicant's independent claims that recite and require a transparent proxy. This is so, because the client in Makarios must not only be aware of the proxy but must register with that proxy and include an initial profile or configuration. A user of the client must even provide a handle name or user name before interaction with that proxy can commence. See, Makarios, col. 5 lines 10-17. This is a specific teaching of a "forward proxy" and not a "transparent proxy," as is recited in Applicant's independent claims. With a "forward proxy" a client is preconfigured and is aware of interactions with the proxy that acts on its behalf. This is what specifically occurs and is taught in the Makarios reference. With a "transparent proxy" the client is totally unaware of the presence and

actions of the proxy and is not preconfigured to interact with it. Thus, the Makarios reference cannot work with a "transparent proxy service."

With respect to this argument, the Examiner asserted in the Advisory that "the test for obvious is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references . . . [;r]ather the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art." Advisory Action, mailed January 24, 2006.

Applicant respectfully asserts that the Examiner has taken the law out of context and incorrectly applied it in this case. Specifically, there must be a motivation to combine the reference; references cannot just be combined at random and then used to assert that the combined teachings teach the limitations of the Applicant's invention. To provide meets and bounds on this the Courts have established a variety of rules and the Patent Office has also promulgated a number of rules.

First, the courts have said that any proposed combination is improper when it teaches away from one or more of the other references used in the combination. *In re Grasselli*, 713 F. 2d 731, 743 (Fed. Cir. 1983). In the instant case, the Makarios reference teaches a forward proxy and the Green reference teaches a transparent proxy. Thus, the combination is improper because they teach away from one another and therefore it is unlikely that one of ordinary skill in the art would have had any motivation to combine the two references.

Second, the courts have said that if a reference teaches away from the invention or the proposed combination renders the primary reference unsatisfactory for its intended purpose than the combination and/or reference is improper. *In re Gurley*, 27 F. 3d 551, 554 (Fed. Cir. 1994). Here, Makarios requires a user registration with the proxy it therefore cannot work with a transparent proxy, thus the Makarios reference teaches away from Applicant's novel transparent proxy service and teaches away from the Green reference; in addition, if Makarios included a transparent proxy it would be inoperable. Therefore, the proposed combination is unlikely again because one of ordinary skill in the

art would not have read Makarios and Green and had motivation to combine them in the manner proposed by the Examiner.

Third, the courts have said that proposed modification cannot run contrary to accepted wisdom in the arts. *In re Hedges*, 783 F.2d 1038 (Fed. Cir. 1986). One of ordinary skill in the art recognizes the difference between processing and architectural setup for a forward proxy versus a transparent proxy. The technique presented in Makarios is heavily reliant on a forward proxy arrangement and requires direct client registration and configuration to establish the initial cookie for a user on the client that the client than actively attaches to requests and forwards to the proxy. All of these actions are indicative of a forward proxy arrangement. The entire teaching of Makarios is lost and is not clear as to how it might even operate if a transparent proxy were used. Therefore, the combination is improper because accepted wisdom would not have considered changing the proxy in Makarios to a transparent proxy, since in doing so Makarios becomes inoperable for its intended purpose.

Fourth, the courts have said that any proposed combination cannot be made if in so doing the principal operation of one of the references is changed. *In re Ratti*, 270 F. 2d 810 (CCPA 1959). Once again, if Makarios were to have a transparent proxy than its teachings will not operate in their intended manner and the principles of the core teachings of Makarios are lost. Thus, the combination is improper and should be withdrawn.

Fifth, the courts have consistently said that an Examiner cannot make a combination via improper hindsight. *In re McLaughlin*, 443 F. 2d 1392 (CCPA 1971). Here, the Applicant respectfully submits the Examiner performed improper hindsight in combining Makarios with Green because the teachings of Makarios rely on a forward proxy and its advantages for what Makarios is attempting to achieve and Green relies on a transparent proxy and its advantages for what Green is attempting to achieve. One of ordinary skill in the art would not have combined the transparent proxy of Green with Makarios because Makarios becomes non operational and one of ordinary skill in the art would not have combined the forward proxy of Makarios with Green because then Green loses its primary teaching of transparent connection validation for applications. Thus,

Applicant believes the only motivation available to combine the two references could have only been acquired after reading and comprehending Applicant's invention and the motivation to combine cannot be acquired from the Applicant's disclosure. Thus, the motivation to combine the references is lacking and is only existent as a result of improper hindsight acquired from reading Applicant's invention. Thus, the proposed combination is improper and should be withdrawn.

Applicant respectfully submits that two unrelated references cannot just be grabbed and asserted because the combined teaches of the two are said to include each and every limitation. It has always been the case and the law that references can only be combined with proper foundation including motivation and there are litanies of situations for which combinations of references are in fact legally impermissible. Applicant asserts that such is the case here and that the references have been improperly combined and that the claims are allowed since the primary reference Makarios cannot be modified with a transparent proxy or it loses its core principles. Thus, Applicant requests that the rejections be withdrawn.

D. The Other Rejections Under 35 U.S.C. § 103(a):

Claims 4-6, 18-19, and 29-31 were rejected as being unpatentable over Makarios and Green in view of several other references. These claims are dependent from the independent claims discussed above. Therefore, Applicant asserts that these claims should be allowed in view of the arguments presented above with respect to the independent claims.

8. SUMMARY

It is respectfully submitted that the art cited does not render the independent claims of record obvious and that the claims are patentable over the cited art. Therefore, reversal of the rejections and allowance of the pending claims are respectfully requested.

Respectfully submitted,

HASHEM M. EBRAHIMI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date 04/06/06 By Joseph P. Mehrle
Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 6 day of April, 2006.

Peter Rehfeldt
Name

Peter Rehfeldt
Signature

CLAIMS APPENDIX

1. (Rejected) A method for brokering state information exchanged between computers using at least one protocol above a transport layer, the method comprising the steps of:

receiving at a transparent proxy a request from a client requesting a resource of an origin server, wherein the transparent proxy is unknown to the client;

redirecting the client request from the transparent proxy to a policy module;

obtaining at the transparent proxy policy enforcement data, wherein the policy enforcement data is received from the policy module and wherein the policy module and the transparent proxy reside within a same environment;

generating at the transparent proxy a policy state token in response to the policy enforcement data; and transmitting the policy state token from the transparent proxy to the client, wherein the policy state token is used as an authentication of the client to the transparent proxy for subsequent interactions between the client and the transparent proxy.

2. (Rejected) The method of claim 1, further comprising the step of receiving at the transparent proxy a renewed request for the origin server resource, the renewed request containing the policy state token.

3. (Rejected) The method of claim 2, wherein the renewed request contains the policy state token in a cookie in a header sent from the client to the transparent proxy.

4. (Rejected) The method of claim 2, further comprising the step of forwarding to the origin server a portion of the renewed request, the forwarded portion omitting the policy state token.

5. (Rejected) The method of claim 4, further comprising the step of receiving at the transparent proxy a reply from the origin server, the reply containing an origin state token for use by the proxy in its subsequent communications with the origin server.

6. (Rejected) The method of claim 4, further comprising the steps at the transparent proxy of forwarding to the client at least a portion of a communication from the origin server, and forwarding to the origin server at least a portion of a communication from the client.

7. (Rejected) The method of claim 1, wherein HTTP is a protocol used during at least one of the receiving and transmitting steps.

8. (Rejected) The method of claim 1, wherein HTTPS is a protocol used during at least one of the receiving and transmitting steps.

9. (Rejected) The method of claim 1, wherein the method further comprises utilizing Novell Directory Services software to provide authentication information about the client, and the transparent policy enforcement data obtained by the transparent proxy depends on the authentication information thus provided.

10. (Rejected) The method of claim 1, wherein the method further comprises utilizing Lightweight Directory Access Protocol software to provide authentication information about the client, and the policy enforcement data obtained by the transparent proxy depends on the authentication information thus provided.

11. (Rejected) The method of claim 1, wherein the method further comprises utilizing Secure Sockets Layer software to provide authentication information about the

client, and the policy enforcement data obtained by the transparent proxy depends on the authentication information thus provided.

12. (Rejected) The method of claim 1, wherein the obtaining step extracts policy enforcement data from a redirection address field.

13. (Rejected) The method of claim 1, wherein the transmitting step transmits the policy state token in a cookie in a header sent from the transparent proxy to the client.

14. (Rejected) A transparent proxy server comprising:

a memory configured at least in part by a transparent proxy process;

a processor for running the transparent proxy process;

at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand; and

a policy module identifier which identifies a policy module that grants or denies authorization of proxy services to the client computer by acquiring policy enforcement data and attempting to authenticate the client computer to the transparent proxy process in response to the policy enforcement data, and wherein the client computer directs a request for a resource to an origin server and the request is intercepted by the transparent proxy process, which is unknown to the client computer, and used to determine the policy module identifier which identifies the policy module, and wherein the policy module authenticates the client computer to the transparent proxy process for subsequent interactions between the client computer and the transparent proxy process, and wherein the policy module processes within a same environment as the transparent process.

15. (Rejected) The transparent proxy server of claim 14, in combination with the policy module.

16. (Rejected) The transparent proxy server of claim 15, wherein the policy module and the transparent proxy process are running on the same computer.

17. (Rejected) The transparent proxy server of claim 14, in combination with the client computer and at least one other client computer, each client computer linked for networked communication with the transparent proxy process.

18. (Rejected) The transparent proxy server of claim 14, wherein the transparent proxy server provides authorized proxy service transparently to both the client computer and the origin server by steps which comprise receiving the request from the client for the resource of the origin server, sending the client computer an authorization by the policy module for the client computer to use a transparent proxy service, accepting the authorization from the client computer with a renewed client request for the origin server resource, forwarding the renewed client request to the origin server without forwarding the authorization but with an indication to the origin server that the transparent proxy server is the source of the forwarded request, and then transparently forwarding the requested resource from the origin server to the client computer.

19. (Rejected) The transparent proxy server of claim 18, wherein the transparent proxy server send the client computer the authorization by sending the client computer a proxy cookie for use in subsequent communications from the client computer.

20. (Rejected) The transparent proxy server of claim 14, in combination with at least one additional transparent proxy server which also has a memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, a link, and a policy module identifier.

21. (Rejected) The combined transparent proxy servers of claim 20, wherein one transparent proxy server forwards other client requests to the other transparent proxy server.

22. (Rejected) The combined transparent proxy servers of claim 20, wherein one transparent proxy server takes over the handling of client requests in place of the other transparent proxy server.

23. (Rejected) A pair of state information brokering signals embodied in a distributed computer system, the system containing a client, a transparent proxy server having a transparent proxy server address, and a policy module having a policy module address, the pair of signals comprising:

a first signal including a redirection command which specifies the policy module address as a redirection target; and

a second signal including a redirection command which specifies the transparent proxy server address as a redirection target and also including policy enforcement data which grants or denies authorization for the client to use a service of the transparent proxy server, and wherein the transparent proxy server controls access to the service based on client authentication to the proxy service achieved through the policy enforcement data, the first and second signal originating within a same environment that is external to the client, and wherein the transparent proxy server is unknown to the client.

24. (Rejected) The signal pair of claim 23, wherein the first signal includes an identity broker address as the policy module address.

25. (Rejected) The signal pair of claim 23, wherein the first signal includes a login server address as the policy module address.

26. (Rejected) The signal pair of claim 23, wherein the second signal includes the policy enforcement data embedded in an address field with the transparent proxy server address.

27. (Rejected) A computer storage medium having a configuration that represents data and instructions which will cause performance of method steps for transparent proxy services, the method comprising the steps of:

receiving at a transparent proxy a request from a client requesting a resource of an origin server, wherein the transparent proxy is unknown to the client;

redirecting the client request from the transparent proxy to a policy module; and

obtaining at the transparent proxy policy enforcement data provided by the policy module, the policy enforcement data granting or denying authorization for the client to access the resource through the transparent proxy, wherein the policy enforcement data is directed to authenticating the client to the transparent proxy and the transparent proxy vends access to the resource, and wherein the policy module and the transparent process execute within a same environment that is external to the client.

28. (Rejected) The configured storage medium of claim 27, wherein the policy enforcement data grants authorization for the client to access the resource through the transparent proxy, and the method further comprises the steps of generating at the transparent proxy a proxy cookie containing at least a portion of the policy enforcement data, and transmitting the proxy cookie from the transparent proxy to the client.

29. (Rejected) The configured storage medium of claim 28, wherein the method further comprises the steps of accepting the proxy cookie at the transparent proxy with a renewed client request for the origin server resource, and forwarding the renewed client request to the origin server without the proxy cookie.

30. (Rejected) The configured storage medium of claim 29, wherein the method further comprises the step of transparently forwarding the requested resource from the origin server to the client.

31. (Rejected) The configured storage medium of claim 27, wherein the transparent proxy is a first transparent proxy, the policy enforcement data includes first policy enforcement data which grants authorization for the client to access the resource through the first transparent proxy, and the method further comprises the steps of:

generating at the first transparent proxy a proxy cookie in response to the first policy enforcement data;

transmitting the proxy cookie from the first transparent proxy to the client;

receiving the first proxy cookie from the client at a second transparent proxy with a renewed client request for the origin server resource, after the first transparent proxy becomes unavailable to the client;

redirecting the renewed client request from the second transparent proxy to a policy module; and

accepting, at the second transparent proxy, the second policy enforcement data provided by the policy module, the second policy enforcement data including authorization from the policy module for the client to access the resource through the second transparent proxy.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.